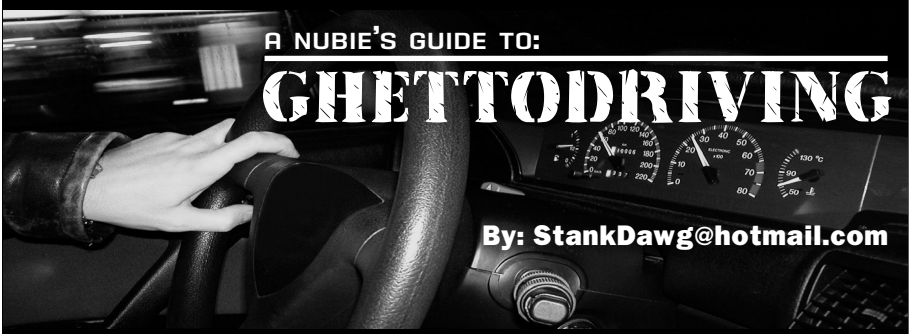

A NUBIE'S GUIDE TO:

GHETTODRIVING

By: StankDawg@hotmail.com

INTRODUCTION:

Back in the early days of hacking, we had a term called "Wardialing" which referred to the act of dialing large sequences of phone numbers with a modem with the hopes of finding an open modem on the other line. If a modem picked up, you would then see what kind of access you had on the other end, and try to access the computer on the other end. Now, a new form of the same style of attack has appeared. It is called "Wardriving".

Wardriving is the act of driving around in a car, with a wireless access card, and looking for open wireless networks. Wardriving has a subset known as "Ghettodriving". Ghettodriving is aterm first coined by dual_parallel of the Digital DawgPound (DDP) and quickly adopted by the rest of us. It refers specifically to a very quick and inexpensive version of wardriving. Basically, "we of the ghetto" cannot always afford the most expensive laptops, wireless cards, and antennas (which is very important in increasing the range of your scanning). Ghettodriving is about making due with what you have. This is a guide to how to get out and about and ghettodriving with a low initial cost as quickly and easily as possible.

STEP 1: HARDWARE

Ok, first of all, you need a laptop. It does not have to be a powerful system! You can find a used laptop for 500 bucks and it will most likely work. All it needs is a way to pick up wireless signals. That can be through PCMCIA cards or USB adapters. If you really want to get technical, you could actually use a full sized desktop and monitor if you really wanted to lug it out into your car. This would require a special power setup to maintain power to such a large machine, and basically drives up the price. This defeats the purpose of ghettodriving. It will also make it more obvious to you and get you busted easier.

In addition to a cheap laptop, you will need a device to pick up the wireless signals. Most commonly, this will be a wireless PCMCIA card. Generally, most cards are supported by the latest versions of the software (see "STEP 2" below) but you can always check it out on the web before you purchase one. If you are using Windows XP, which is what this guide is mostly geared towards, you have a better chance of the card working since generic drivers for Windows XP are available.

Another possibility is to use a USB wireless adapter from your USB device. I have tried this and it does work. The benefit is that older laptops may not have PCMCIA slots. You also simply may not want to purchase a PCMCIA card for whatever reason. I had a USB adapter for my home network, and I used it for ghettodriving until I was able to purchase a PCMCIA card. The obvious drawback here is that you have this bulky USB cable and adapter hanging off of the side of your laptop. It is not a big deal to get started, or if you are truly driving and not moving or picking the laptop, but eventually, you will want to stop somewhere and use the laptop and the extra piece of hardware will annoy the hell out of you. Especially if you get out of the car and begin "warwalking".

GPS (Global Position System) devices are a luxury that Ghettodrivers can forego. These devices will add extra information to your Ghettodriving. Specifically, they can add latitude and longitude readings for each wireless network you find. This is helpful to pinpoint the exact location of networks that you pick up. Usually, you will know your own scans and save them with well chosen filenames to make them recognizable. When you start sharing your information with others (see STEP 5), they may need more precise information.

Antennas are another optional step, but these are generally unused by ghettodrivers. They are sometimes expensive, and the point of ghettodriving is to keep the cost down. You can find many places one the web to research how to make your own antenna, but it will require some time and knowledge. A better alternative for the ghettodriver with a budget would be to purchase on of the models of PCMCIA cards that has an opening for an external antenna built onto the edge of the card. Both Orinoco and Cisco make models like this with many more companies following suit.

STEP 2: SOFTWARE

Again, since this is geared for nubies, I am going to focus on the Windows XP environment. The software of choice for Windows XP is called "Network Stumbler" or "NetStumbler" for short. Always download the latest version to assure support for the greatest number of cards. Also, do not worry if your card is listed under the unsupported list. As I said earlier, Windows XP and NetStumbler provide generic drivers that may detect your card just fine even if it is not listed as a supported card.

There are also good clients for Linux. The most notable is "Kismet". If you are familiar with Linux, this might be the best way to go since Linux also has a few more tools and utilities for cracking. If you do not want to commit your entire laptop to Linux, you can also try the Knoppix distribution, which boots and runs entirely from the CD.

Also, since ghettodriving is about making due with what you have, I would be remiss to mention what do to if your card is not supported by NetStumbler or Kismet. Since Windows XP wireless networking is set to always listen for WAPs anyway, you may simply need the client application software that came with your wireless card. With this installed and running, you can simply use the built-in Windows XP wireless support to find wireless networks. There are other packages like aphopper that may work in a pinch as well. It is not as friendly as having a dedicated app like NetStumbler, but it will work, and that is the bottom line.

NetStumbler installation is straightforward. Once you install the software, you simply start the application and it will begin "sniffing" for Access Points. As you move around, and come in and out of range of wireless network, NetStumbler will detect and notify you of the network. At this point, you are up and running, but it is important that you understand a few more things before you go further.

STEP 3: UNDERSTAND HOW IT WORKS

Wireless Access Points, or WAPs (or even simply APs) work on radio frequencies using basic radio wave technology. It is not much different than the way that your car radio works. Radio stations send out an extremely strong signal that gets picked up by your car radio (thus the need for an antenna). This is the same way that wireless networking works, only on a smaller scale. The radio station has a set frequency that you dial in on your radio tuner and it is sent out from an enormous broadcasting tower. A Wireless Access Point sends out a constant signal at a set frequency. The only real difference is that 802.11 has a much smaller range.

Since you know that the WAP is shouting out its availability all the time, just like a radio station, common sense tells you that you must be able to dial into that frequency, just like a

radio station. You got it exactly! That is the fundamental principal in Wardriving. The programs mentioned in the software section above are simply listening devices that are tuning in to the 802.11 frequency and waiting for that signal (or station) to come in. When you come within the vicinity of an Access Point, it lets you know.

The software will indicate to you when it has found a wireless network shouting its availability. Since you have a wireless card, and they have a wireless access point, you can now become a user on their network. There are a few more details and or restrictions as explained below, but in the simplest form, and in a basic insecure (and very common) setup, you will have full access to the network!

STEP 4: ACCESS!

What does that mean? Well, there are some factors that can establish and/or limit what access you do have, but generally, you will have a lot of access to that network. When a typical home user sets up their home network, they are doing it for the purpose of having easy and convenient access to the internet. A typical business will set up their wireless network to be both easy to maintain and easy to access for its employees. To that end, they usually leave the access point wide open so that when they set up computers in their home or business, they can easily set it up and be off and running. Their laziness is our gain.

When you drive or walk into the wireless network range, you are no different than a computer sitting in their office. Most of these networks have DHCP turned on and anyone connecting to the network gets a generic DHCP address assigned to their computer for routing purposes. With that address, you are now a node in their network. If they have internet access turned on, which they almost always do, you have the ability to sit in their parking lot and surf the web or check your email on their bandwidth.

There is an exception to this rule. There always is. In the example I just walked you through; we made a lot of assumptions on availability. These assumptions are true in more than 50% of networks that I have found. Sometimes, however, you will find that the person has turned on WEP (Wired Equivalent Privacy) encryption. WEP encryption requires that all client systems on a network know the WEP key to gain access to the network. Think of it as a long password. For Ghettodriving purposes, WEP enabled networks mean that you shouldn't even bother with that network. There are software packages that will attempt to crack WEP encryption, but Ghettodrivers are usually just looking for quick access. If WEP is enabled, it is easier to simply find another wireless network without WEP turned on and use it instead.

There is another reason that Ghettodrivers don't usually bother with WEP enabled networks. It is a legal issue. While it is currently legal to locate and acknowledge the existence of wireless networks, it is ILLEGAL to ACCESS ANY NETWORK WITHOUT PERMISSION! Even if WEP is turned off, it is still illegal to access a network, wireless or otherwise, without permission. Frankly, in most circumstances, it is near impossible to be discovered, but this is not in any way, shape, or form insinuating that you break the law! It is just pointing out a matter of fact. If someone goes to the effort of implementing encryption (and possibly other forms of authentication), they obviously are NOT giving you permission to access their network. This being the case, Ghettodrivers choose to skip them. Even though most Ghettodrivers feel that it is harmless to piggyback on someone else's bandwidth to do a web search for information or to do a quick check of an email account, they will not generally force

their way into a system. It is a grey area that borders a very illegal border, so each person must draw their own lines and set their own limits on how far they will go. The legal line is crossed upon actual access of the network.

Also, just for informational purposes, once you are on a network, you may be curious as to how the network is set up or who the network belongs to (so you can thank them). Since you are another perfectly established node on that network, you can use network tools just like any other network client. Utilities like LANGUARD and AIROPEEK can be wonderful for researching the network. You might come up with many other creative ways to use your newfound access, but again BE CAREFUL. You may be doing something that, while it can be harmless, may technically be illegal.

STEP 5: RESULTS

As you Ghettodrive, your results are maintained onscreen until you close the program. Once a network has been found, you can save the information to a file which you can access later. Maybe you take a trip to Disneyworld once per year. Each time you go back, you now know the locations of places to access the internet without starting all over again. Or you can share the file with a friend who is going also. You may have the need to jump online and lookup prices for something from the parking lot of a store before your purchase. You may want to check for an email from friends regarding where they want to meet you in the park. The uses are endless!

You can also upload the results of your Ghettodriving to many different sites online. Instead of giving a list of these sites, you will be better of to simply go online and search for sites that you prefer, perhaps something local. Sharing with a few friends is useful, but can you imagine sharing information with the whole world? Not only will your friend know where to go, but now, so will anyone else who wants to visit Disneyworld! People can get online before buying tickets and make sure the reseller is legitimate and not a con artist. Publicly releasing information will actually raise the consciousness of society. I'll bet some of you reading this never realized that hacking can produce such awareness and contribute to the betterment of society on such a grand scale. Maybe hackers aren't so bad after all!

CONCLUSION:

In summary, this is one of the most fun things to do since Wardialing. Finding places to get internet access in such strange places as parking lots and highways is an amazing feeling. If you understand how it works, and know where they lines are, you can safely, and legally, explore the world on a whole new level. You will never look at your neighborhood the same again!